L-3 Communications

Privatel™ Model 960v

FIPS 140-1 Non-Proprietary

Cryptographic Module Security Policy

Date: 20 September, 2000

Prepared By: Ron Paraggio
L-3 Communication Systems - East
One Federal Street
Camden, New Jersey 08103

TABLE OF CONTENTS

1 Overview

1.1 Purpose

This document is a non-proprietary Cryptographic Module Security Policy for the L-3 Communications Privatel™ Model 960v voice encryption module. This policy was prepared as part of the Privatel™ FIPS 140-1 certification. The Privatel™ Model 960v provides superior security, meeting all FIPS 140-1 level 1 requirements and many of the level 2 requirements.

1.2 Description

The Privatel™ Model 960v is a multiple-chip standalone cryptographic module that provides security for voice telephony applications. The Privatel™ product is an applique to an existing office telephone that provides voice coding, traffic encryption, key management, and modem functions. Privatel™ is compact, very easy to use, and provides users with portable secure communications from virtually any office, home, or private telephone. The module uses the strongest commercially available cryptography, which provides end-to-end secure communications that protect telephone conversations from eavesdropping and unauthorized monitoring and recording. The module displays a unique Key Fingerprint during every secure session to ensure that there are no unauthorized listeners. In addition to the excellent security features, Privatel™ uses a toll quality vocoder providing excellent voice quality, making secure calls nearly transparent.

1.3 Additional Information

For more detailed information about the Privatel™ Model 960v, please visit the Privatel™ web site at http://www.L-3com.com/privatel. The web site contains a detailed product description, specifications, FAQ's, information about telephone security, and contacts.

For answers to sales or technical questions please refer to the contacts listed on the Privatel™ web site at http://www.L-3com.com/privatel, or call Toll Free 877-628-3694, or E-mail: privatel@L-3com.com.

For more information about the FIPS 140-1 standard and validation program please visit the NIST web site at http://csrc.nist.gov/cryptval.

2 Roles and Services

The Privatel™ supports two separate roles, a Crypto Officer role and a user role. The Crypto Officer role is performed during manufacturing process when the Privatel™ is being assembled and the user role is performed by the person who operates the module as an end user.

2.1 Crypto Officer Role

The Crypto Officer is responsible for initializing the Privatel™ with Key Exchange Vectors and PIN Based Access Control, which enable the end user to operate the module. The Key Exchange Vectors consist of Diffie-Hellman algorithm parameters necessary for the Privatel™ to perform a public key based generation of a traffic encryption key. The Key Exchange Vectors are loaded into the module during the assembly process and cannot be modified by the user in the field.

2.2 User Role

The User of the Privatel™ is responsible for the proper operation of the module. The User must verify the appropriate state of the Privatel™ when it is being used for secure communications. In addition to verifying the Privatel's™ secure mode indication he must also verify with the far-end user that the Key Fingerprint displayed on both modules are identical.

2.3 Crypto Officer Services

The Crypto Officer services are performed during the manufacturing process before the Privatel™ assembled. The Crypto Officer can exercise the following services:

Set Key Exchange Vectors
Initialize/Reset PIN Based Access Control

2.4 User Services

The User can exercise the following services:

Initiate transition from Non-Secure Mode to Secure Mode
Initiate transition from Secure Mode to Non-Secure Mode
Enable PIN
Disable PIN
Change PIN
Adjust Receive Audio Level
Secure Mute
Select Phone Type
Run Self-Test

3 Rules of Operation

This section contains a description of the Privatel™ rules of operation. The basic operations covered in this section are:

1) Placing unencrypted non-secure telephone calls, 2) Securing a telephone call, 3) Adjusting the earpiece volume while in a secured call, 4) Muting the microphone while in a secured call, 5) Enabling and disabling the Personal Identification Number (PIN) based Access Control feature of the Privatel™, 6) Changing the PIN, and 7) Performing a self-test on the Privatel™.

3.1 Non-Secure Telephone Calls

Non-secure calls can be placed whenever the Privatel™ is powered off, or when its display reads "Non-Secure Mode". Non-secure calls can be placed even in the event of a power failure. The Privatel™ does not have to be disconnected from your telephone in order to place a non-secure call.

3.2 Securing a Telephone Call

To place a secure call, perform the following steps:

1. Pick-up your telephone's handset and dial your phone normally. Make sure that your Privatel™ is turned on and displaying "Non-Secure Mode." Next, ensure that the far-end party has a Privatel™ connected to his/her phone and that their Privatel™ is also powered on.
2. Set your telephone's handset volume control, if present, to its normal (middle) position.
3. Agree on which one of you will press the SECURE/NONSEC key to initiate secure mode.

IMPORTANT: *Only one* party may initiate secure mode

4. To enter secure mode, press the SECURE/NONSEC key on the Privatel™. [If the far-end party is the initiator, you should not press the SECURE/NONSEC key.] If PIN-based access control is enabled, enter your 4-digit PIN when requested. The display will then show, in sequence, these messages: "Establishing Connection", "Training Secure Modem", and "Exchanging Key Parameters" to indicate the status of the security establishment process. Voice communications will be blocked while the Privatel™ is securing your phone call.
5. After 8 to 15 seconds, the top line of the Privatel™ display will change to "SECURE MODE". This indicates that the call is secured. The bottom line of the display will change to "Key Print" followed by a 5-digit Key Fingerprint number. Verify that this number appears.
6. Ask the far-end party to read the 5-digit Key Fingerprint displayed on their Privatel™. If their Key Fingerprint is identical to your Key Fingerprint, then the call is secured. If the Key Fingerprints are not identical, press the SECURE/NONSEC key and repeat steps 3 through 6. If the Key Fingerprints continue to differ from each other, then your call is most likely under a cryptographic attack by a malicious third party and your privacy may be compromised. If you find yourself in this situation, you and the far-end party should both attempt to move to different locations before trying to place another secure call.
7. To return to non-secure mode, <u>one</u> party must press the SECURE/NONSEC key (this need not be the same party that initiated the transition to secure mode). The other party will then be alerted by the presence of a non-secure warning tone (3 beeps in rapid succession). The Privatel™ will briefly display a message indicating that it is transitioning to non-secure mode. When the transition is complete, the display will read, "Non-Secure Mode".

8. Occasionally, drastic changes in telephone line conditions can occur during a typical phone call. If this happens the Privatel™ may not be able to maintain line security, in which case it will alert both users with a non-secure warning tone (3 beeps in rapid succession) and briefly display "Signal Lost Going Non-Secure" before reverting to non-secure mode. At this point, steps 3 through 7 should be repeated in order to re-establish security.

3.3 Adjusting Receive Audio Level

To decrease the earpiece**{** XE "earpiece volume" **}{** XE "receive volume" **}** (receiver) volume of a secure call, press the 3 (VOL-) key. To increase the earpiece (receiver) volume of a secure call, press the 4 (VOL+) key. During volume adjustment, the Privatel™ will display a bar graph indicating the current volume setting. These settings only apply when the Privatel™ is operating in secure mode, and are retained even after power is removed. As a general rule, use the volume controls on your telephone during a normal non-secure conversation and the volume controls on your Privatel™ during a secure conversation.

3.4 Secure Mode Mute

If you wish to mute**{** XE "mute" **}** your microphone during a secure call, press the 0 (MUTE) key. The display will read, "*Muted*" and the far-end party will not be able to hear you. To return to normal operation, press the 0 (MUTE) key again. The display will return to the normal secure mode display. As a general rule, use the mute control on your telephone during a normal non-secure conversation and mute control on your Privatel™ during a secure conversation.

3.5 PIN-Based Access Control

The Privatel™ provides PIN Based Access Control for user authentication. The user can enable, disable, and change the PIN. Only the crypto officer can reset the PIN if it is forgotten.

1.1.1 Enabling PIN-Based Access Control{ XE "Access Control" }

The Privatel™ can be configured to require the entry of a 4-digit Personal Identification Number**{** XE "Personal Identification Number" \t "*See* PIN" **}** (PIN**{** XE "PIN" **}**) prior to enabling secure communications. To enable this feature, press the MENU key, then repeatedly push the NEXT key until the top line of the display reads, "→ ENABLE PIN." Now press the ENTER key and type in the four digit PIN you wish to use via the 0-9 Keys. You will be asked to repeat the new PIN to ensure correctness.

3.5.2 Disabling PIN-Based Access Control

PIN-based access control can be disabled again via the menu. To disable PIN access, press the MENU key, then repeatedly push the NEXT key until the top line of the display reads, "→ DISABLE PIN." Now press the ENTER key and type in your four digit PIN to authorize the request. If the PIN you enter is not correct, PIN-based access control will remain enabled.

3.5.3 Changing the PIN

If PIN-based access control is enabled, you can change your four-digit PIN to a new value. To change the PIN, press the MENU key, then repeatedly push the NEXT key until the display reads, "→ CHANGE PIN." Press the ENTER key and type in the old PIN for authorization, then type in the new four-digit PIN you wish to use using the 0-9 keys. You will be asked to repeat the new PIN to ensure correctness.

WARNING: THERE IS NO WAY TO RESTORE OPERATION IF YOU FORGET YOUR PIN! IT IS STRONGLY RECOMMENDED THAT YOU WRITE DOWN YOUR SELECTED PIN AND KEEP IT IN A SAFE PLACE AWAY FROM YOUR PRIVATEL™.

3.6 Performing a Self-Test{ XE "Self-Test" }

Your Privatel™ automatically performs a self-test whenever it is powered on. A self-test can also be activated via the menu when in non-secure mode. To perform this self-test, press the MENU pushbutton, then repeatedly push the NEXT key until the top line of the display reads, "→ SELF TEST." Next, press the ENTER key. After a few seconds, the display will present the results of the self-test.

3.7 Physical Security

The Privatel™ cryptographic module is contained within an opaque, impact resistant, cycoloy grade plastic enclosure that is screwed together. Privatel™ is a FIPS 140-1 level 1 module, so there are no physical security requirements or rules.

4 Key Management

4.1 Generic Key Management

The Privatel™ contains non-volatile memory (NVM) for keying (and other) parameters which are 'durable', and volatile memory for transient parameters which are only associated with one cryptographic session.

The Privatel™ checks its Key Exchange Vectors stored in NVM upon each power-up and upon each self-test to ensure data integrity. Fields with errors shall be actively overwritten.

If, after NVM checking, the Privatel™ does not contain a Key Exchange Vector, a self-test failure is reported to the user and secure operations are disabled.

The Privatel™ actively erases all transient parameters (Session Key, subkeys, etc.) and unencrypted parameters upon the termination of a cryptographic session. These transient and unencrypted parameters are only stored in internal, volatile memory.

4.2 Initial Default State

Upon assembly, the Privatel's™ non-volatile memory will be pre-programmed with the Key Exchange Vector(s) in place.

4.3 Start-up Keying

The Key Exchange Vectors are stored in plain format in the non-volatile memory.

4.4 Session Key Development Algorithm

The Privatel™ derives the Session Key using the Diffie-Hellman based Session Key Development Algorithm (SKDA). Each module randomly generates a one-time, secret value "*i*", and transmits to the far-end module the value Y_i in the Session Setup Message, where,

$$Y_i = (g^{i}) \bmod p.$$

The values *g* and *p* are shared and are not secret. The parameter *g* shall be less than *p*. The length of *p* is 1024 bits.

A Privatel™ will receive from the far-end terminal the value Y_j, where *j* is the far-end terminal's random, one-time, secret value, and Y_j is

$$Y_j = (g^{j}) \bmod p.$$

Each SOCS terminal shall verify that the received value of Y is less than *p*, otherwise the secure call is terminated. The SOCS terminal then calculates

$$W = ((g^{j}) \bmod p)^{i} \ \ mod\ p).$$

The far-end SOCS terminal performs the similar calculation,

$$W = ((g^{i}) \bmod p)^{j}\ mod\ p).$$

The results of these two calculations are identical and provide a number *W* with length *p*. This number is then manipulated to produce a traffic key.

4.4.1 Conversion to a Traffic Key

To convert the Diffie-Hellman result *W* into a traffic key, the following steps are performed. First, the field W is reduced using the Secure Hash Algorithm (SHA-1), resulting in a 168 bit traffic key and a 16 bit Key Fingerprint. This Key Fingerprint is displayed to the user in decimal format for verification to prevent a man-in-the middle attack.

4.4.2 Cryptographic Algorithm

The Privatel™ uses the Triple DES algorithm in output feedback mode for traffic encryption.

4.4.3 Key Distribution

Key exchange vectors are loaded into the Privatel™ via the Factory Initialization Interface when the unit is assembled in the factory.

4.4.4 Key Entry

The Privatel™ does not support key entry by the user.

The Privatel™ supports key exchange vector entry (the base and the modulus) via the Factory Initialization Interface when the unit is assembled in the factory. The exponent is randomly generated every call.

4.4.5 Key Storage

The Privatel™ provides non-volatile storage for three complete sets of key exchange parameters (the base and the modulus; the exponent is randomly generated per call).

When in any state other than going secure or secure mode, no unprotected key information (traffic key or Diffie-Hellman exponent) resides in the Privatel.

Unprotected key information (traffic key or Diffie-Hellman exponent) never resides outside of the microprocessor/DSP device, which is utilizing the information.

4.4.6 Key Destruction

Upon any transition from secure mode to a non-secure mode, the Privatel™ actively erases the traffic key, any expanded traffic key values, all results of the Diffie-Hellman exchange, and the Diffie-Hellman private key.